UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

THOMAS PIKE and **ANDREW HAWKINS**, on behalf of themselves and all others similarly situated, Plaintiffs, vs. **FLAGSTAR BANK**, Defendant.	Case No. 2:22-11642

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Thomas Pike and Andrew Hawkins ("Plaintiffs"), individually and on behalf of the proposed class and subclass defined below, bring this action against Defendant Flagstar Bank ("Flagstar"), and allege as follows:

I. SUMMARY OF THE ACTION

1. This action stems from Flagstar's failure to secure the sensitive personal information of its customers. For the second time in less than 2 years, sensitive personal information belonging to Flagstar customers has been compromised by an unauthorized party.

2. Between December 3, 2021 and December 4, 2021, an unauthorized actor accessed Flagstar's network ("The Data Breach"). Flagstar did not learn of the breach until six months later on June 2, 2022. The impacted files contained names, phone numbers, and Social Security numbers. The Data Breach impacted

over 1.5 million customers.

3. As a result of Flagstar's data security failures, Plaintiffs and Class members confront a significant threat of identity theft and other harm – imminently and for years to come. Plaintiffs by this action seek compensatory damages together with injunctive relief to remediate Flagstar's failure to secure their PII, and to provide credit monitoring, identity theft insurance, and credit repair services to protect the class of Data Breach victims from identity theft and fraud.

II. PARTIES

4. Plaintiff Thomas Pike is a citizen of Coto De Caza, California. His mortgage was previously acquired by Flagstar. After refinancing, Mr. Pike received notice from Flagstar of a data breach that occurred in December 2020. Mr. Pike repeatedly called Flagstar to remove his information from their systems. On June 22, 2022, Mr. Pike received a subsequent letter from Flagstar notifying him of a second data breach, stating that certain files containing his personal information had been accessed and/or acquired from Flagstar's network. Mr. Pike experiences stress and anxiety from concerns that he faces an increased risk of identity theft, fraud, and other types of monetary harm.

5. Plaintiff Andrew Hawkins is a citizen of Meridian, Idaho. Around June 17, 2022, Mr. Hawkins received a letter from Flagstar informing him that

files containing his personal information had been accessed and/or acquired from Flagstar's network. Mr. Hawkins experiences stress and anxiety from concerns that he faces an increased risk of identity theft, fraud, and other types of monetary harm.

6. Defendant Flagstar Bank was chartered in 1987 as a federal savings bank. It now has assets of $31 billion and is the sixth largest bank mortgage originator, and the second largest savings bank, in the United States. Flagstar's principal place of business is located at 5151 Corporate Drive, Troy, Michigan.

III. JURISDICTION AND VENUE

7. This Court has jurisdiction over the lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332, because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of class members exceed $5,000,000, exclusive of interest, attorneys' fees, and costs; and (3) Flagstar and class members are domiciled in different states.

8. The Court has personal jurisdiction over Flagstar because its principal place of business is within this District and it has sufficient minimum contacts in Michigan to render the exercise of jurisdiction by this Court proper and necessary.

9. Venue is proper in this District under 28 U.S.C. § 1391(b) because Flagstar is headquartered in this District and because a substantial part of the

events or omissions giving rise to the claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Customers Trust Flagstar with Their PII

10. Flagstar provides banking and lending services. Customers must provide Flagstar with their personally identifiable information ("PII"), including Social Security numbers, first and last names, and phone numbers to bank with Flagstar.

11. On its website, Flagstar recognizes that "[t]he war against cyber criminals is fought daily as attacks become more difficult to detect and stop," and there is "no way to predict the damage that can be caused by a single cyber attack."[1] Flagstar knows that "identity fraud affects 17 million people on an annual basis" and that its customers entrust it with their "data and information that is valuable to cyber criminals."

12. Flagstar advises its customers to follow "10 cyber security tips to safeguard against potential online threats." The second of Flagstar's cyber security tips is: "update your software." Flagstar emphasizes the importance of "mak[ing] sure your programs are up to date and running the latest version."

13. Plaintiffs and Class members reasonably expected that Flagstar would keep their PII confidential and would not make unauthorized disclosures

[1] https://www.flagstar.com/financial-resource-center/cyber-safety.html (last visited July 8, 2022).

of this information. Plaintiffs and Class members relied upon Flagstar to securely maintain their PII and to adopt and maintain security measures that would prevent its involuntary disclosure.

14. Flagstar did not implement reasonable cyber security measures and failed to take appropriate steps to protect and secure the personal information of its customers.

Flagstar's Files Are Breached by Cyber Criminals

15. On June 17, 2022, Flagstar began mailing notices of the Data Breach to affected persons.

16. In the letter, Flagstar states that they "recently experienced a cyber incident that involved unauthorized access" to their networks.

17. Between December 3 and December 4, 2021, an unauthorized actor accessed Flagstar's network. Flagstar did not discover the breach until June 2, 2022.

18. Information exposed in the Data Breach includes names, phone numbers, and Social Security numbers.

19. In the letter, Flagstar advised customers to take protective measures, such as reviewing accounts frequently, signing up for credit monitoring, placing fraud alerts, and requesting a credit freeze.

20. Social Security numbers and other PII are valuable to criminals. This

information can be and has been sold and traded on the dark web black market.

21. The loss of a Social Security number is particularly troubling because it cannot easily be changed and can be misused in a range of nefarious activities, such as filing fraudulent tax returns to steal tax refund payments, opening new accounts to take out loans, and other forms of identity theft.

22. While Flagstar has offered two years of credit monitoring services from Kroll, the offer is inadequate because it will not protect Plaintiffs and Class members after those first two years, even though their personal information will still be in the hands of cyber criminals. Criminals often wait for a year or more before using stolen data for identity theft, and once the personal information is posted online, opportunities for misuse will multiply and extend into the future.

Flagstar Had Foreseeable Vulnerabilities

23. As early as 2009, Flagstar was the subject of a data security breach when one of its vendor's laptops containing Social Security numbers of its customers was stolen.

24. Then, in December 2020 and January 2021, a legacy file transfer application used by Flagstar was breached, compromising the PII of nearly 1.5 million Flagstar customers and employees. The stolen information included names, Social Security numbers, account numbers, phone numbers, and addresses. The provider of the file transfer application described it as a "20 year

old product nearing end-of life" and stated it had "encouraged all FTA customers to migrate to kiteworks."[2] Flagstar failed to heed these warnings.

25. Hackers also targeted Flagstar with ransom demands, posting Social Security numbers and home addresses of Flagstar employees taken in the breach.

26. Flagstar knew that safeguarding the PII of its customers is of the utmost importance. Over the past several years, data breaches like the incursion into Flagstar's electronic systems have occurred and been reported on in the news.

Plaintiffs' Injuries

27. Each Plaintiff has suffered anxiety and mental distress resulting from Flagstar's failure to secure his or her PII, reasonably fearing identity theft resulting from the Data Breach. Each Plaintiff faces a materially heightened risk of the unauthorized opening of new financial and other accounts in his or her name, now and in the future. According to the Federal Trade Commission's Consumer Sentinel Network, in 2020 there were nearly 1.4 million reports of identity theft received through the FTC's identitytheft.gov website, about twice as many as in 2019.[3] Of those reports, over 400,000 came from people who said their information was misused to apply for a government document or benefit, up

[2] https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited July 11, 2022)

[3] https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

from some 23,000 in 2019.[4] According to a report by Javelin Strategy & Research, identity theft cost Americans a total of about $56 billion in 2020.[5]

28. As reported in the Detroit Free Press, Adam Levin, founder of CyberScout and author of a book on identity theft, "said that if criminals do publish Social Security numbers and other personal information, the victims of hacks like that affecting Flagstar customers are at high risk of tax fraud, tax refund diversion, fraudulent unemployment claims and fraudulent new account creation schemes, among other bad things."[6]

29. Each Plaintiff has lost the ability to control how his or her PII is used; experienced a concomitant diminution in the value of that PII; faces future costs in the form of time, effort, and money to be expended to prevent, detect, contest, and repair the adverse effects of the theft of his or her PII in the Data Breach; and faces a heightened risk that his or her PII remaining in Flagstar's possession will be compromised in the future due to inadequate measures and systems to protect same.

V. CLASS ACTION ALLEGATIONS

30. Plaintiffs bring this lawsuit as a class action on their own behalf and

---

[4] *Ibid.*

[5] *See*: https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html.

[6] https://www.freep.com/story/money/business/michigan/2021/03/24/flagstar-bank-customers-information-breach-accellion/6987681002/.

on behalf of all other persons similarly situated, pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements of Rule 23. The Class and Subclass are defined as:

> **Class**
> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Flagstar Bank on or about June 17, 2022 (the "Nationwide Class").

> **California Subclass**
> All individuals residing in California whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Flagstar Bank on or about June 17, 2022 (the "California Subclass").

Plaintiffs reserve the right to modify, change, or expand the Class definition, including proposing additional subclasses, based on discovery and further investigation.

Numerosity and Ascertainability

31. The number of Class members is so large as to make joinder impracticable. Flagstar has reported that over 1.5 million persons were affected by the Data Breach.

32. The identities and contact information of Class members are readily ascertainable from information and records in the possession, custody, or control of Flagstar. Notice of this action can be readily provided to the Class.

Typicality

33. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised in the Data Breach.

Adequacy of Representation

34. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interest contrary to or in conflict with the interests of Class members.

Predominance of Common Issues

35. Common questions of law and fact exist as to all members of the Class and predominate over any questions pertaining only to individual Class members. Among the questions of law and fact common to the Class are:

a. Whether Flagstar had a duty to implement reasonable cyber security measures to protect Plaintiffs' and Class members' sensitive, personal information and to promptly alert them if such information was compromised;

b. Whether Flagstar breached its duties by failing to take reasonable precautions to protect Plaintiffs' and Class members' sensitive, personal information;

c. Whether Flagstar acted negligently by failing to implement adequate data security protocols and otherwise act to secure the sensitive, personal information entrusted to it;

d. Whether Flagstar violated the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*.

e. Whether Flagstar's failures to implement reasonable data security protocols and to timely notify Plaintiffs and Class members of the Data Breach violate the Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq*.

f. Whether Flagstar unlawfully invaded Plaintiffs' and Class members' privacy by recklessly allowing the Data Breach to occur through its inaction;

g. What relief is warranted for Plaintiffs and the Class under the circumstances; and

h. The appropriate measure of damages for the breach victims.

Superiority

36. A class action is superior to all other available methods for resolving this controversy. Absent a class action, most Class members would likely find the cost of pursuing their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class members' claims, few, if any, Class members would seek redress for Flagstar's violations.

37. Class wide adjudication of common questions of law and fact will conserve the resources of the courts and promote efficiency and consistent results.

Generally Applicable Conduct

38. Class wide injunctive and corresponding declaratory relief is appropriate under Rule 23(b)(2), as Flagstar acted and failed to act in a manner that applies generally to the Class.

FIRST CAUSE OF ACTION

Negligence

39. Plaintiffs incorporate and reallege the foregoing allegations of fact.

40. Plaintiffs assert this claim on behalf of themselves and the Class.

41. Flagstar collected, stored, and transferred the personal information of Plaintiffs and Class members, including their Social Security numbers, first and last names, and telephone numbers.

42. Flagstar owed Plaintiffs and Class members a duty of reasonable care to preserve and protect the confidentiality of their personal information that it collected. This duty included, among other obligations, maintaining and testing its security systems and computer networks, using up-to-date and secure versions of file transfer software, and taking other reasonable security measures to

safeguard and adequately secure the personal information of Plaintiffs and Class members from unauthorized access and use.

43. Plaintiffs and Class members were the foreseeable victims of Flagstar's inadequate cybersecurity. The natural and probable consequence of Flagstar's failing to adequately secure its information networks was the hacking of Plaintiffs' and Class members' personal information.

44. Flagstar knew or should have known that Plaintiffs' and Class members' personal information was an attractive target for cyber thieves, particularly in light of data breaches that Flagstar and other entities experienced. The harm to Plaintiffs and Class members from exposure of their highly confidential personal facts was reasonably foreseeable to Flagstar.

45. Flagstar had the ability to sufficiently guard against data breaches by implementing adequate measures to protect its systems.

46. Flagstar breached its duty to exercise reasonable care in protecting Plaintiffs' and Class members' confidential personal information by failing to implement and maintain adequate security measures to safeguard the information, failing to monitor its systems and files to identify suspicious activity, and allowing unauthorized access to and exfiltration of the information.

47. There is a close connection between Flagstar's failure to employ reasonable security protections for its customers' personal information and the

injuries suffered by Plaintiffs and Class members. When individuals' sensitive personal information is stolen, they face a heightened risk of identity theft and need to: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries and charges; (5) place and renew credit fraud alerts on a quarterly basis; (6) contest fraudulent charges and other forms of identity theft; (7) repair damage to credit and financial accounts; and (8) take other steps to protect themselves and attempt to avoid or recover from identity theft and fraud.

48. Flagstar also owed a duty to timely disclose to Plaintiffs and Class members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiffs and Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5)

intensively monitor loan data and public records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

49. Flagstar breached its duty to timely disclose the Data Breach to Plaintiffs and Class members. Flagstar did not discover the breach until six months after the Data Breach occurred. Flagstar unreasonably delayed in notifying Plaintiffs and Class members of the Data Breach. That unreasonable delay caused foreseeable harm to Plaintiffs and Class members by preventing them from taking timely self-protection measures in response to the Data Breach.

50. The policy of preventing future harm necessitates the finding that Flagstar had an independent duty in tort to protect this data and thereby avoid reasonably foreseeable harm to Plaintiffs and class, particularly given the extremely sensitive data entrusted to Flagstar.

51. As a result of Flagstar's negligence, Plaintiffs and Class members have suffered damages in an amount to be determined at trial. Those damages include or may include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) diminution in the value and use of their personal information entrusted to Flagstar; (3) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (4) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased

costs to use credit, credit scores, credit reports, and assets; (5) unauthorized use of compromised personal information to open new financial and other accounts; (6) continued risk to their personal information, which remains in Flagstar's possession and is subject to further exposure for as long as Flagstar fails to undertake appropriate and adequate measures to protect the personal information in its possession; (7) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach; and (8) anxiety and mental distress resulting from the foreseeable and reasonable fear that they may become victims of identity theft due to Flagstar's failure to adequately protect their PII.

SECOND CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 Civ. Code § 1798.100 et seq. (CCPA)

52. Plaintiffs incorporate and reallege the foregoing allegations of fact.

53. Plaintiff Pike asserts this claim on behalf of himself and the California Subclass.

54. Section 1798.150(a)(1) of the CCPA provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Civil Code section 1798.81.5(d)(1)(A)] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate

to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the Court deems proper.

55. Plaintiff Pike is a consumer and California resident as defined by Civil Code section 1798.140(g).

56. Flagstar is a "business" as defined by Civil Code section 1798.140(c) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California." Flagstar has annual gross revenues in excess of $25 million. Flagstar annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, householders, or devices.

57. Plaintiff Pike's and California Subclass members' personal information, as defined by Civil Code section 1798.81.5(d)(1)(A), was subject to unauthorized access and exfiltration, theft or disclosure. The Data Breach described herein exposed, without limitation, Social Security numbers, first and

last names, and telephone numbers.

58. The Data Breach occurred as a result of Flagstar's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Flagstar failed to monitor its files to identify suspicious activity, failed to upgrade to a more secure cyber security system, even after a previous data breach less than two years earlier, and allowed unauthorized access to Plaintiff Pike's and California Subclass members' PII.

59. Consistent with Civil Code section 1798.150(b)(1), Plaintiff Pike provided written notice to Flagstar identifying the CCPA provisions Flagstar violated on [DATE]. If Flagstar is unable to cure or does not cure the violations within 30 days, Plaintiff will amend this complaint to pursue actual or statutory damages as permitted by section 1798.150(a)(1)(A) of California's Civil Code.

60. Plaintiff presently seeks injunctive and declaratory relief, and any other relief deemed appropriate by the Court, for Flagstar's CCPA violations.

THIRD CAUSE OF ACTION

Violation of the Unfair Competition Law, Bus. & Prof. Code § 17200 *et seq.* (UCL)

61. Plaintiffs incorporate and reallege the foregoing allegations of fact.

62. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. &

Prof. Code § 17200.

63. Flagstar's conduct is unlawful, in violation of the UCL, because it violates the CCPA.

64. Flagstar's conduct is fraudulent because it omitted, suppressed, and concealed material facts regarding its failure to take reasonable or adequate precautions to secure Plaintiff Pike's and California Subclass members' personal information. Despite being aware of vulnerabilities in their system—which Plaintiff and California Subclass members had no reasonable means of knowing—Flagstar did not disclose this information to Plaintiff or California Subclass members.

65. Flagstar's conduct also is unfair and deceptive in violation of the UCL. Flagstar's unfair and fraudulent business acts and practices include:

a. failing to adequately secure the personal information of Plaintiff and California Subclass members from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about Plaintiff and California Subclass members in a manner highly offensive to a reasonable person;

c. enabling the disclosure of personal and sensitive facts about Plaintiff and California Subclass members without their informed, voluntary,

affirmative, and clear consent; and

d. unreasonably delaying discovery of the Data Breach, and therefore delaying notice of the Data Breach, preventing Plaintiff and California Subclass members from taking timely self-protection measures.

66. The gravity of harm resulting from Flagstar's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

67. The harm from Flagstar's conduct was not reasonably avoidable by consumers. The individuals affected by the Data Breach were required to provide their names, telephone numbers, and Social Security numbers as part of their relationship with Flagstar. Plaintiff and California Subclass members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures.

68. There were reasonably available alternatives that would have furthered Flagstar's business interests of electronically storing their customers' information while protecting PII, such as upgrading their security system and ensuring best practices in cybersecurity defense.

69. Flagstar's omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability

to protect the confidentiality of Plaintiff's and California Subclass members' personal information. A reasonable person would regard Flagstar's derelict data security and the Data Breach as important, material facts. Flagstar could and should have timely disclosed these facts.

70. As a direct and proximate result of Flagstar's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and California Subclass members lost money or property because their sensitive personal information experienced a diminution of value and because they devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to monitoring their credit reports and financial accounts for fraudulent activity.

71. Plaintiff and California Subclass members therefore seek all monetary and non-monetary relief permitted by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs under Code of Civil Procedure section 1021.5.

FOURTH CAUSE OF ACTION

Invasion of Privacy

72. Plaintiffs incorporate and reallege the foregoing allegations of fact.

73. Plaintiffs assert this claim on behalf of themselves and the Class.

74. Flagstar wrongfully intruded upon Plaintiffs' and Class members'

seclusion. Plaintiffs' and Class members reasonably expected that the personal information they entrusted to Flagstar—such as their Social Security numbers, first and last names, and phone numbers —would be kept private and secure, and would not be disclosed to any unauthorized third party or for any improper purpose.

75. Flagstar unlawfully invaded Plaintiffs' and Class members' privacy rights by:

a. failing to adequately secure their personal information from disclosure to unauthorized third parties or for improper purposes;

b. enabling the disclosure of personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

76. A reasonable person would find it highly offensive that Flagstar, having received, collected, and stored Plaintiffs' and Class members' names, Social Security numbers, and other personal details, failed to protect that information from unauthorized disclosure to third parties.

77. In failing to adequately protect Plaintiffs' and Class members' personal information, Flagstar acted knowingly and in reckless disregard of their privacy rights. Flagstar experienced a data breach, less than two years prior, but

failed to upgrade to a more secure cybersecurity system. Flagstar knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' positions.

78. Flagstar violated Plaintiffs' and Class members' common law right to privacy, which includes the right to control their personal and private information.

79. Flagstar's unlawful invasions of privacy damaged Plaintiffs and Class members. As a direct and proximate result of these violations, Plaintiffs and Class members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for an order:

A. certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel to represent the Class;

B. entering judgment for Plaintiffs and the Class;

C. awarding Plaintiffs and Class members monetary relief;

D. ordering appropriate injunctive relief;

E. awarding pre- and post-judgment interest as prescribed by law;

F. awarding reasonable attorneys' fees and costs as permitted by law; and

G. granting such further and other relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 15, 2022

Respectfully submitted,

/s/ *Michael N. Hanna*
Michael N. Hanna (P81462)
MORGAN & MORGAN, P.A.
2000 Town Center, Suite 1900
Southfield, MI 48075
(313) 251-1399
mhanna@forthepeople.com

Adam E. Polk (CA State Bar No. 273000)
Simon Grille (CA State Bar No. 294914)
Jessica Cook (CA State Bar No. 339009)
GIRARD SHARP LLP
601 California St, Ste 1400
San Francisco, CA 94108
Phone: (415) 981-4800
apolk@girardsharp.com
sgrille@girardsharp.com
jcook@girardsharp.com

Attorneys for Plaintiffs